CLAIMS

What is claimed is:

1. A method comprising:

associating cryptography information with a data packet to be used to perform cryptography operations on the data packet;

storing the cryptography information in memory;

generating a pointer to a memory location for the cryptography information;

passing the pointer to the cryptography information from a first system layer to a second system layer;

accessing the cryptography information not stored in the second system layer using the pointer;

performing cryptography operations on the data packet; and

transmitting the data packet.

2. The method of claim 1 wherein the first system layer comprises an intermediate driver agent.

3. The method of claim 1 wherein the second system layer comprises a base driver agent.

4. The method of claim 1 wherein the cryptography information comprises one or more of: a unique identifier, a network protocol associated with the data packet, a security parameter index, cryptographic keys, a source identifier, and a destination identifier.

5. The method of claim 1 wherein the cryptography information comprises a security association.

6. The method of claim 1 wherein the pointer is used to cache the cryptography information on network hardware.

7. The method of claim 1 wherein accessing the cryptography information not stored in the second system layer is performed by the second system layer to populate a cryptography information table.

8. The method of claim 7 wherein the population of the cryptography information table is performed when cryptography information for the data packet is needed for network hardware to perform cryptography operations on the data packet.

9. A method comprising:

receiving a data packet;

associating cryptography information with the data packet, the cryptography information to be used to perform cryptography operations on the data packet;

generating a message indicating that the cryptography information necessary to perform cryptography operations on the data packet is not stored in a cryptography information table; and

passing the message from a first system layer to a second system layer.

10. The method of claim 9 wherein the first system layer comprises a base driver agent.

11. The method of claim 9 wherein the second system layer comprises an intermediate driver agent.

12. The method of claim 9 wherein the cryptography information comprises one or more of: a unique identifier, a network protocol associated with the data packet, a security parameter index, cryptographic keys, a source identifier, and a destination identifier.

13. The method of claim 9 wherein the cryptography information comprises a security association.

14. The method of claim 9 further comprising the second system layer passing cryptography information to the first system layer to populate the cryptography information table.

15. The method of claim 14 wherein the second system layer passing cryptography information to populate the cryptography information table occurs only as the cryptography information is needed to perform cryptography operations on a data packet.

16. The method of claim 9 wherein passing the message causes the second system layer to determine which of multiple methods of data packet processing should be used to process the data packet.

17. An article comprising a machine-accessible medium to provide machine-readable instructions that, when executed, cause one or more electronic systems to:

associate cryptography information with a data packet to be used to perform cryptography operations on the data packet;

store the cryptography information in memory;

generate a pointer to a memory location for the cryptography information;

pass the pointer to the cryptography information from a first system layer to a second system layer;

access the cryptography information not stored in the second system layer using the pointer;

perform cryptography operations on the data packet; and

transmit the data packet.

18. The article of claim 17 wherein the pointer is used to cache the cryptography information on network hardware.

19. The article of claim 17 wherein accessing the cryptography information not stored in the second system layer is performed by the second system layer to populate a cryptography information table.

20. The article of claim 19 wherein the population of the cryptography information table is performed when cryptography information for the data packet is needed for network hardware to perform cryptography operations on the data packet.

21. An article comprising a machine-accessible medium to provide machine-readable instructions that, when executed, cause one or more electronic systems to:

receive a data packet;

associate cryptography information with the data packet, the cryptography information to be used to perform cryptography operations on the data packet;

generate a message indicating that the cryptography information necessary to perform cryptography operations on the data packet is not stored in a cryptography information table; and

pass the message from a first system layer to a second system layer.

22. The article of claim 21 further comprising the second system layer passing cryptography information to the first system layer to populate the cryptography information table.

23. The article of claim 22 wherein the second system layer passing cryptography information to populate the cryptography information table occurs only as the cryptography information is needed to perform cryptography operation on the data packet.

24. The article of claim 21 wherein passing the message causes the second system layer to determine which of multiple methods of data packet processing should be used to process the data packet.

25. An electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising sequences of instructions that, when executed, cause one or more electronic systems to:

associate cryptography information with a data packet to be used to perform cryptography operations on the data packet;

store the cryptography information in memory;

generate a pointer to a memory location for the cryptography information;

pass the pointer to the cryptography information from a first system layer to a second system layer;

access the cryptography information not stored in the second system layer using the pointer;

perform cryptography operations on the data packet; and

transmit the data packet.

26. The electronic data signal of claim 25 wherein the pointer is used to cache the cryptography information on network hardware.

27. The electronic data signal of claim 25 wherein accessing the cryptography information not stored in the second driver agent is performed by the second system layer to populate a cryptography information table.

28. The electronic data signal of claim 27 wherein the population of the cryptography information table is performed when cryptography information for the data packet is needed for network hardware to perform cryptography operations on the data packet.

29. An electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising sequences of instructions that, when executed, cause one or more electronic systems to:

receive a data packet;

associate cryptography information with the data packet, the cryptography information to be used to perform cryptography operations on the data packet;

generate a message indicating that the cryptography information necessary to perform cryptography operations on the data packet is not stored in a cryptography information table; and

pass the message from a first system layer to a second system layer.

30. The electronic data signal of claim 29 further comprising the second system layer passing cryptography information to the first system layer to populate the cryptography information table.

31. The electronic data signal of claim 30 wherein the second system layer passing cryptography information to populate the cryptography information table occurs only as the cryptography information is needed to perform cryptography operations on a data packet.

32. The electronic data signal of claim 29 wherein passing the message causes the second system layer to determine which of multiple methods of data packet processing should be used to process the data packet.

33. An apparatus comprising a first system layer coupled to a second system layer, the first system layer to store cryptography information in memory, and to generate and to pass to the second system layer a pointer to cryptography information stored in memory, the cryptography information necessary to perform cryptography operations on a data packet, the second system layer to access the cryptography information not stored in the second system layer using the pointer.

34. The apparatus of claim 33 wherein the first system layer comprises an intermediate driver agent.

35. The apparatus of claim 33 wherein the second system layer comprises a base driver agent.

36. The apparatus of claim 33 wherein the pointer is used to cache the cryptography information on network hardware.

37. The apparatus of claim 33 wherein accessing the cryptography information not stored in the second system layer is performed by the second system layer to populate a cryptography information table.

38. The apparatus of claim 37 wherein the population of the cryptography information table is performed when cryptography information for the data packet is needed for network hardware to perform cryptography operations on the data packet.

39. An apparatus comprising a first system layer coupled to a second system layer, the first system layer to generate a message indicating that cryptography information necessary to perform cryptography operations on a data packet is not stored in a cryptography information table, and to pass to the second system layer the message.

40. The apparatus of claim 39 wherein the first system layer comprises a base driver agent.

41. The apparatus of claim 39 wherein the second system layer comprises an intermediate driver agent.

42. The apparatus of claim 39 further comprising the second system layer passing cryptography information to the first system layer to populate the cryptography information table.

43. The apparatus of claim 42 wherein the second system layer passing cryptography information to populate the cryptography information table occurs only as the cryptography information is needed to perform cryptography operations on the data packet.

44. The apparatus of claim 39 wherein passing the message causes the second system layer to determine which of multiple methods of data packet processing should be used to process the data packet.